

U.S. DISTRICT COURT  
DISTRICT OF VERMONT  
FILED

2021 JAN 19 PM 12:48

CLERK

BY AW  
DEPUTY CLERKUNITED STATES DISTRICT COURT  
FOR THE  
DISTRICT OF VERMONT

UNITED STATES OF AMERICA )

v. )

SEAN FIORE, )

Defendant. )

Case No. 2:19-cr-00078-1

**OPINION AND ORDER  
DENYING DEFENDANT'S MOTION TO SUPPRESS EVIDENCE FOR LACK  
OF PROBABLE CAUSE**

(Doc. 36)

Pending before the court is Defendant Sean Fiore's motion to suppress evidence found during the execution of a search warrant at his residence on May 17, 2019. (Doc. 36.) He contends the search warrant was stale and therefore not supported by probable cause in violation of the Fourth Amendment to the United States Constitution. He further contends that the executing officers' reliance on the search warrant was not objectively reasonable and thus cannot be excused by the good faith exception to the exclusionary rule articulated in *United States v. Leon*, 468 U.S. 897 (1984).

In an October 20, 2020 hearing, Defendant asked to cross-examine the officers who executed the search warrant regarding their good faith. The court granted leave to file a supplemental memorandum to address whether good faith is determined by an objective or subjective standard. *Id.* at 922 (holding that the exclusionary rule should not apply when evidence is "obtained in objectively reasonable reliance on a subsequently invalidated search warrant[.]"). Defendant's supplemental memoranda do not squarely address this issue. Instead he argues that under *Franks v. Delaware*, 438 U.S. 154 (1978), the court should hold an evidentiary hearing requiring the government to establish the executing officers' objective reasonableness in relying on the search warrant. The government opposes the motion.

The government is represented by Assistant United States Attorneys Barbara A. Masterson and Mona N. Sahaf. Defendant is represented by Maryanne E. Kampmann, Esq. and Robert L. Sussman, Esq.

Defendant is charged in a Third Superseding Indictment alleging: (1) intent that a murder be committed in violation of 13 V.S.A. §§ 2301 and 2311 and 18 U.S.C. § 956 pursuant to 18 U.S.C. § 1958(a); (2) knowing receipt of child pornography in violation of 18 U.S.C. §§ 2252(a)(2) and 2252(b)(1); (3) knowing possession of child pornography in violation of 18 U.S.C. §§ 2252(a)(4)(B) and 2252(b)(2); (4) conspiring to commit kidnapping and murder outside the United States in violation of 18 U.S.C. §§ 956(a)(1) and 956(a)(2)(A); (5) conspiring to entice any minor to engage in production of child pornography in violation of 18 U.S.C. §§ 2251(a) and 2251(e); (6) enticing any minor to engage in production of child pornography in violation of 18 U.S.C. §§ 2251(a) and 2251(e); and (7) knowingly receiving, aiding and abetting, and attempting to receive child pornography in violation of 18 U.S.C. §§ 2252(a)(2) and 2252(b)(1), (2).

**I. Factual Background.**

The following facts are derived from Homeland Security Investigations Special Agent Caitlin Moynihan's May 9, 2019 affidavit in support of her search warrant application.

**A. BitTorrent.**

BitTorrent is a peer-to-peer ("P2P") file sharing software that allows users to share files directly with other BitTorrent users. P2P software also allows a user to download multiple files at the same time from different computers, thereby increasing download speeds. To access P2P software, "a user must first obtain the P2P software, which can be downloaded from the Internet." (Doc. 36-1 at 20.) During the installation of P2P software, a user may be able to reconfigure certain default settings including designating which folders on his or her computer will be made available to other BitTorrent users for download. "It is the computers linked together through the Internet using [P2P] software that form the BitTorrent network that allows for the sharing of digital files between users." *Id.* at 21.

“To share . . . files on the BitTorrent network, a ‘Torrent’ file needs to be created by the user that initially wants to share a file or set of files.” *Id.* at 22. A Torrent is a small file that describes the file being shared, including how to locate the file, however, a Torrent does not actually contain that file. “Once a Torrent is created, in order to share the file(s) referenced in the Torrent file, a user typically makes the Torrent available to other users, such as via websites on the Internet.” *Id.*

A user may locate Torrent files of interest by conducting a keyword search on a Torrent indexing website, such as isohhunt.com or thepiratebay.org. “Torrent indexing websites are essentially search engines that users on the BitTorrent network use to locate Torrent files that describe the files they are looking to download.” *Id.* at 23.

After a user locates a Torrent file he or she wishes to download on an indexing website, the user must download the Torrent file to his or her computer and “[t]he BitTorrent program on the user’s computer will then process that Torrent file in order to find users . . . on the network that have all or part of the file(s) referenced in the Torrent file.” *Id.* “The actual file(s) referenced in the ‘Torrent’ are obtained directly from other users . . . on the BitTorrent network. This means the download of a file is achieved through a direct connection between the computer requesting the file and the computer(s) sharing the actual file(s)[.]” (Doc. 36-1 at 23.) “[A]s users download files or pieces of files from other peers/clients of the BitTorrent network, other users . . . on the network are able to download the files or pieces of files from them, a process which maximizes the download speed for all users on the network.” *Id.* at 21-22. Once a user has completed the download, he or she can share the file with other individuals using the BitTorrent network, a process referred to as “seeding.” *Id.* at 22 (internal quotation marks omitted).

With BitTorrent, users must affirmatively select files for download and files cannot be sent from one computer to another without the recipient’s permission. While running BitTorrent, users can view the Internet Protocol (“IP”) addresses of the users with whom they share files. An IP address is a “unique numeric address used by computers on the Internet. . . . Every computer attached to the Internet must be assigned

an IP address so that Internet traffic sent from and directed to that computer may be directed properly[.]” *Id.* at 30.

Once a file is downloaded using BitTorrent, it will be stored in a previously designated area on the user’s computer where it “will remain until moved or deleted.” *Id.* at 23.

**B. Characteristics of Child Pornographers.**

Special Agent Moynihan avers that certain characteristics are common to child pornographers:

c. Those who produce, distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes often possess and maintain copies of child-pornography material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home, or in some other secure location.

d. Likewise, those who produce, distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area.

*Id.* at 19.

**C. Special Agent Moynihan’s Single Source Download.**

On March 25, 2019, Special Agent Moynihan used “investigative BitTorrent software[.]” and connected directly to IP address 98.229.2.46 for fifty minutes. (Doc. 36-1 at 24.) She connected to that IP address because it was associated with a Torrent referencing “a file of investigative interest to child pornography investigations.” *Id.* IP address 98.229.2.46 was the sole candidate for Special Agent Moynihan’s download and while connected to it, she accessed a file titled “1st-Studio Siberian Mouse HD\_125(M-11).wmv” (“Siberian Mouse”). *Id.* (internal quotation marks omitted). The download provided her with access to an eighteen minute and forty-one second video. Although “[o]nly portions of the video play[ed,]” *id.*, Special Agent Moynihan was able to view the file during the download and determined that it depicted “two nude pubescent female children, approximately 12-14 years old, on what appears to be a bed[,]” with one child



performing oral sex on a dildo and the other child touching her genital area with a vibrator. *Id.* at 24-25.

“Files of investigative interest are files that have been previously identified by law enforcement officers as files containing child exploitative material based on their SHA values.” *Id.* at 24. “SHA[-]1 hash values” are identifiers “also known as digital signatures” that are used as “evidence verification in electronic discovery and computer forensics.” (Doc. 36-1 at 22 n.1.) An SHA-1 hash value represents a unique image file because it is “computationally infeasible to find two different files which produced the same hash value when run through . . . [a] one-way mathematical algorithm.” *Id.*

Special Agent Moynihan averred that the Siberian Mouse file, or evidence thereof, was likely to be recovered from a computer associated with IP address 98.229.2.46 because:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on a storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

*Id.* at 32.

**D. Special Agent Moynihan's Investigation of the IP Address 98.229.2.46.**

The day after her single source download of the Siberian Mouse video, on March 26, 2019, Special Agent Moynihan searched publicly available records and determined that IP address 98.229.2.46 was serviced by Comcast. On April 10, 2019, after serving Comcast with a subpoena for subscriber information for the IP address, Special Agent Moynihan learned that the IP address was registered to 92 Overlake Park, Apt. 2, Burlington, Vermont. She also confirmed that the IP address's subscriber/user was Defendant. Thereafter, Special Agent Moynihan requested information regarding Defendant from the Vermont Intelligence Center and determined that he was born in 1983. She conducted a records check in the Federal Bureau of Investigation Interstate Identification Index and searched the State of Vermont's criminal history databases for information about Defendant, which yielded no results.

On April 12, 2019, Special Agent Moynihan requested the names of persons receiving mail at 92 Overlake Park, Apt. 2, Burlington, Vermont from the United States Postal Service ("USPS") and determined that Lillian Kimball, Mara Coven, Defendant, and Aude Fiore received mail at that address. That same day, Special Agent Moynihan sought records from the Vermont Department of Motor Vehicles ("DMV") regarding any vehicles and drivers associated with the Overlake Park address. The DMV responded that Lillian Kimball, Mara Coven, Defendant, and Aude Fiore each had a car registered to that address, a driver's license associated with that address, or both. The DMV provided photographs of each of these individuals. On April 17, 2019, Special Agent Moynihan caused a summons to be sent to the Vermont Department of Labor requesting wage information related to Defendant and received a response that he had been employed by the University of Vermont Nursing and Health Sciences since 2018.

**E. Investigative Efforts to Determine Defendant's Residence.**

On April 16, 2019, Special Agent Mike McCullagh visited 92 Overlake Park, Burlington, Vermont at 0610 hours and observed no lights on in the residence. He saw a vehicle bearing the license plate FRY588 parked in the driveway and determined that this license plate was registered to Defendant. Special Agents Moynihan and McCullagh

returned to 92 Overlake Park at 1534 hours that same day and observed no vehicles in the driveway. They photographed the premises and noted that there were no address markings near a door which appeared to provide access to a garage.

On April 23, 2019, Special Agent Moynihan returned to the 92 Overlake Park address and observed no vehicles. She asked USPS for information regarding where mail for Apartment 2 was delivered. USPS responded that the apartment was not approved and there was only one mailbox for the building.

Special Agent McCullagh spoke with Bill Ward, the Director of Code Enforcement for the City of Burlington, who indicated that 92 Overlake Park is a single-family residence with no permits authorizing its use as a multi-use residence. On May 8, 2019, Lieutenant Daniel Gamelin of the Chittenden County Sheriff's Department visited the 92 Overlake Park address and while at the front of the residence "observed a male and a female come from the walkway along the left side of the garage to the residence, when facing the residence from Overlake Park. [He] recognized the male as [Defendant] from his DMV photo." *Id.* at 29. He spoke with Defendant and the female and learned that 92 Overlake Park is comprised of three apartments and that Defendant and the female lived in the apartment to the left, the landlord occupied the middle unit, and there was an additional unit to the right. The next day, on May 9, 2019, Special Agent Moynihan sought and obtained a search warrant for Defendant's residence which was required to be executed on or before May 23, 2019. On May 17, 2019, a search of Defendant's residence took place and yielded incriminating evidence.

## **II. Conclusions of Law and Analysis.**

Defendant contends that the facts contained in Special Agent Moynihan's affidavit were stale because she waited six and a half weeks from her download of the Siberian Mouse video to apply for a search warrant. He argues that it was unlikely that the Siberian Mouse video remained on his computer during this time period and that Special Agent Moynihan's affidavit provides no evidence identifying him as someone who is likely to hoard child pornography.

The Fourth Amendment to the United States Constitution provides that:



The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. CONST. amend. IV.

Probable cause exists when, “based on the totality of circumstances, the officer has ‘knowledge of, or reasonably trustworthy information as to, facts and circumstances that are sufficient to warrant a person of reasonable caution in the belief that an offense has been or is being committed[.]’” *Finigan v. Marshall*, 574 F.3d 57, 62 (2d Cir. 2009) (quoting *Zellner v. Summerlin*, 494 F.3d 344, 368 (2d Cir. 2007)). It “is a fluid concept—turning on the assessment of probabilities in particular factual contexts—not readily, or even usefully, reduced to a neat set of legal rules.” *Illinois v. Gates*, 462 U.S. 213, 232 (1983).

In evaluating probable cause, a judge must “make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him [or her], . . . there is a fair probability that contraband or evidence of a crime will be found in a particular place.” *Id.* at 238. “Due to this subjective standard, a reviewing court generally accords ‘substantial deference to the finding of an issuing judicial officer that probable cause exists,’ limiting [its] inquiry to whether the officer ‘had a substantial basis’ for his [or her] determination.” *United States v. Raymonda*, 780 F.3d 105, 113 (2d Cir. 2015) (quoting *United States v. Wagner*, 989 F.2d 69, 72 (2d Cir. 1993)). In making this determination, both the magistrate judge and the reviewing court examine the four corners of the affidavit that supports the warrant application. *United States v. Falso*, 544 F.3d 110, 122 (2d Cir. 2008) (“All data necessary to show probable cause for the issuance of a search warrant must be contained within the four corners of a written affidavit given under oath”) (quoting *United States v. Gourde*, 440 F.3d 1065, 1067 (9th Cir. 2006)) (internal quotation marks omitted).

A court may “conclude that a warrant lacks probable cause where the evidence supporting it is not ‘sufficiently close in time to the issuance of the warrant’ that



‘probable cause can be said to exist *as of the time of the search*[.]’” in other words, “where the facts supporting criminal activity have grown stale by the time that the warrant issues.” *Raymonda*, 780 F.3d at 114 (quoting *Wagner*, 989 F.2d at 72) (emphasis in original). The law recognizes “no bright-line rule for staleness[.]” *Walczyk v. Rio*, 496 F.3d 139, 162 (2d Cir. 2007), however, “the facts in an affidavit supporting a search warrant must be sufficiently close in time to the issuance of the warrant and the subsequent search conducted” so that probable cause continues to exist. *Wagner*, 989 F.2d at 75. The two critical factors in determining staleness are the age of the facts alleged and the “nature of the conduct alleged to have violated the law.” *United States v. Ortiz*, 143 F.3d 728, 732 (2d Cir. 1998) (internal quotation marks omitted).

“[T]he determination of staleness in investigations involving child pornography is ‘unique’” because “‘it is well known that images of child pornography are likely to be hoarded by persons interested in those materials in the privacy of their homes[.]’” *Raymonda*, 780 F.3d at 114 (quoting *United States v. Irving*, 452 F.3d 110, 125 (2d Cir. 2006)). “Crucially, however, the value of that inference in any given case depends on the preliminary finding that the suspect is a person ‘interested in’ images of child pornography.” *Id.* Courts look to a number of factors to infer that a “suspect is a ‘collector’ of child pornography[.]” including, “a suspect’s admission or other evidence identifying him as a ‘pedophile.’” *Id.* They have done so in light of information that the suspect paid for access to child pornography. And they have done so where the suspect has an extended history of possessing or receiving pornographic images. However,

[i]n certain circumstances, courts have even inferred that a suspect was a hoarder of child pornography on the basis of a single incident of possession or receipt . . . where, for example, the suspect’s access to the pornographic images depended on a series of sufficiently complicated steps to suggest his willful intention to view the files. Or they have done so where the defendant, having accessed a single file of child pornography, subsequently redistributed that file to other users.

In all of these cases, the inference that the suspect was a collector of child pornography did not proceed merely from evidence of his access to child pornography at a single time in the past. Rather, it proceeded from circumstances suggesting that he had accessed those images willfully and

deliberately, actively seeking them out to satisfy a preexisting predilection. Such circumstances tend to negate the possibility that a suspect's brush with child pornography was a purely negligent or inadvertent encounter, the residue of which was long ago expunged.

*Id.* at 115 (internal citations omitted).

In *Raymonda*, the Second Circuit considered a staleness challenge in the context of a nine-month delay in the execution of a search warrant after a user's seventeen second access to seventy-six thumbnail images of child pornography on an Internet website. Relying on a forensic investigator's testimony that "images automatically downloaded by a user's web browser are not saved to the user's hard drive, but only to a temporary Internet cache where they typically remain 'two days to a month[,]'" *id.* at 112, the court found the search warrant lacked probable cause based on "nine-month-old evidence[]" that merely "show[ed] that the suspect had at some point access thumbnails of child pornography[]" but "did not even click on any thumbnail links to access the full-sized files." *Id.* at 116-17. It, however, further found that suppression was not warranted because, under *United States v. Leon*, the good faith exception to the exclusionary rule applied.

In this case, the challenged search warrant was issued forty-six days after Special Agent Moynihan downloaded and viewed a file of investigative interest in a child pornography case identified by its SHA-value from an IP address associated with Defendant. She was able to view the Siberian Mouse file and determine for herself that it appeared to contain child pornography. Unlike a file obtained from an Internet website, the Siberian Mouse video was obtained through the use of P2P software that required its recipient to obtain and download the BitTorrent network, search an index using keyword search terms, and affirmatively select the file and download it before it could be shared with others. Because of the way the Siberian Mouse file was obtained, it would not be stored in a temporary Internet cache but would instead be stored in a place designated by the end user unless it was moved or deleted. Even if it was moved or deleted, Special Agent Moynihan averred that forensic artifacts of it were likely to remain on the end user's computer. Special Agent Moynihan obtained the Siberian Mouse video solely from

IP address 98.229.2.46 giving her reason to believe that the subscriber of that IP address had possessed child pornography and shared it.

During the forty-six-day interval between Special Agent Moynihan's single source download of the Siberian Mouse video and the execution of the search warrant, she determined that the IP address from which she obtained it belonged to Defendant. She determined where Defendant lived and took precautions to ensure that only his housing unit was searched. The search warrant was executed eight days after its issuance and fifty-four days after her single source download.

These facts are distinguishable from *Raymonda* for a number of reasons but most importantly because Defendant's "access to the pornographic images depended on a series of sufficiently complicated steps to suggest his willful intention to view the file[]" and he "subsequently redistributed that file" to Special Agent Moynihan. *Raymonda*, 780 F.3d at 115; *see also United States v. Clarke*, 979 F.3d 82, 93-94 (2d Cir. 2020) ("Clarke made use of the BitTorrent peer-to-peer file-sharing network to obtain child pornography files from the computers of others, knowing that by doing so he was enabling other users to obtain the files from his computer" which was sufficient to support a conviction for knowing transportation of child pornography). "Such circumstances tend to negate the possibility that [Defendant's] brush with child pornography was a purely negligent or inadvertent encounter, the residue of which was long ago expunged." *Raymonda*, 780 F.3d at 115.

Of equal importance, the delay in question was a small fraction of the lengthy delay at issue in *Raymonda* and was fully explained by appropriate investigative steps to determine the subscriber of the IP address in question, to determine his criminal history and employment, and to ensure the right residence was searched. Defendant argues that Special Agent Moynihan nonetheless misled the magistrate judge because she failed to acknowledge the possibility that Defendant was downloading the Siberian Mouse video at the exact same moment that she accessed it and further failed to alert him to the possibility that Defendant's download may have been aborted thereafter. Defendant



points out that the search warrant recovered no evidence of the Siberian Mouse file<sup>1</sup> on his computer and the title of the file is not itself indicative of child pornography.

Although it is conceivable that Special Agent Moynihan and Defendant downloaded the Siberian Mouse file simultaneously, probable cause is based not on “hard certainties[.]” but on “assessment of probabilities in particular factual contexts” and requires only a “probability, and not a prima facie showing, of criminal activity[.]” *Gates*, 462 U.S. at 231-32, 235 (internal quotation marks omitted). In any event, probable cause does not require a search warrant affiant to either disclose or rule out all possible innocent explanations for suspicious conduct. *See District of Columbia v. Wesby*, 138 S. Ct. 577, 588 (2018) (holding “probable cause does not require officers to rule out a suspect’s innocent explanation for suspicious facts.”); *United States v. Fama*, 758 F.2d 834, 838 (2d Cir. 1985) (“The fact that an innocent explanation may be consistent with the facts alleged . . . does not negate probable cause. Neither should it preclude a good faith belief in probable cause.”) (internal citations omitted).

For these same reasons, Defendant’s assertion that his alleged single access to the Siberian Mouse video was consistent with “inadvertently stumbling upon” it because he was not able to view the video while it was downloading is equally unpersuasive. The inquiry is not whether a suspect will be arrested and convicted but whether evidence of a particular crime is likely to be found in a particular place. *See United States v. Martin*, 426 F.3d 83, 86 (2d Cir. 2005) (observing “it is untenable to conclude that property may not be searched unless its occupant is reasonably suspected of a crime and is subject to arrest” and that all that is required is to “satisfactorily demonstrate[] to the magistrate that fruits, instrumentalities, or evidence of crime is located on the premises”) (internal

---

<sup>1</sup> The fruits of a search or the lack thereof do not affect the determination of probable cause. *See Florida v. Harris*, 568 U.S. 237, 249 (2013) (“[F]undamentally, we do not evaluate probable cause in hindsight, based on what a search does or does not turn up.”). For this reason, although the Siberian Mouse video was not recovered from Defendant’s computer, this does not negate a finding of probable cause. Correspondingly, the court does not consider the evidence of alleged child pornography found on Defendant’s computer during the search in determining probable cause.



quotation marks omitted). When an IP address is the source of a file with an SHA hash value associated with child pornography, probable cause may be found even without a download. *See United States v. Thomas*, 2013 WL 6000484, at \*23-24 (D. Vt. Nov. 8, 2013) (observing that “hash values provide information regarding a particular file’s contents that is substantially more reliable than a file’s name or size[]” and “[e]ven without a direct download, courts have consistently found probable cause exists when an IP address that appears to have accessed child pornography can be traced to an identifiable residence[]”), *aff’d*, 788 F.3d 345 (2d Cir. 2015); *see also United States v. Cartier*, 2007 WL 319648, at \*2 (D.N.D. Jan. 30, 2007) (concluding search warrant application was supported by probable cause because “hash values [are] a reliable means of investigating child pornography because in practical application, a file’s hash value is unique to that file.”).

Finally, Defendant was not entitled to a *Franks* hearing to establish that a simultaneous download, an aborted download, or the overwriting of the Siberian Mouse file was possible. A *Franks* challenge requires the court:

To determine if the false information was necessary to the issuing judge’s probable cause determination, *i.e.*, material, “a court should disregard the allegedly false statements and determine whether the remaining portions of the affidavit would support probable cause to issue the warrant.” If the corrected affidavit supports probable cause, the inaccuracies were not material to the probable cause determination and suppression is inappropriate.

*United States v. Awadallah*, 349 F.3d 42, 65 (2d Cir. 2003) (quoting *United States v. Canfield*, 212 F.3d 713, 718 (2d Cir. 2000)).

In this case, had Special Agent Moynihan’s affidavit contained Defendant’s purely speculative theory of a simultaneous download of the Siberian Mouse video followed by an aborted download, it would not have altered the existence of probable cause. The Siberian Mouse video was obtained from Defendant’s IP address and thus he arguably possessed it long enough to share it. Special Agent Moynihan’s affidavit addressed in some detail the forensic evidence that might be left behind even if the file was deleted.

The possibility that the file might be overwritten would also be insufficient to defeat probable cause. As the Seventh Circuit has observed:

Because of overwriting, it is *possible* that the deleted file will no longer be recoverable from the computer's hard drive. And it is also *possible* that the computer will have been sold or physically destroyed. And the longer the interval between the uploading of the material sought as evidence and the search of the computer, the greater these possibilities. But rarely will they be so probable as to destroy probable cause to believe that a search of the computer will turn up the evidence sought; for probable cause is far short of certainty—it “requires only a probability or substantial chance of criminal activity, not an actual showing of such activity,” . . . and not a probability that exceeds [fifty] percent (“more likely than not”), either.

*United States v. Seiver*, 692 F.3d 774, 777 (7th Cir. 2012) (emphasis in original).

In reviewing a challenged search warrant, the reviewing court must accord “substantial deference to the finding of an issuing judicial officer that probable cause exists[.]” *Raymonda*, 780 F.3d at 113 (internal quotation marks omitted). The court must consider the totality of the circumstances described in the search warrant affidavit and examine them realistically without insisting on “proof of specific criminal conduct beyond a reasonable doubt or even by a preponderance of the evidence.” *United States v. Martin*, 426 F.3d 68, 76 (2d Cir. 2005).


Here, the search warrant affidavit contained specific facts that supported probable cause for a search warrant of Defendant's residence for child pornography. The information Defendant contends was omitted from Special Agent Moynihan's affidavit would not alter that conclusion. Having concluded that the search warrant was supported by probable cause, the court need not address the application of *Leon*'s good faith exception.

**CONCLUSION**

For the reasons stated above, Defendant's motion to suppress evidence for lack of probable cause is DENIED. (Doc. 36.)

SO ORDERED.

Dated at Burlington, in the District of Vermont, this 19<sup>th</sup> day of January, 2021.

A handwritten signature in black ink, appearing to read 'Christina Reiss', is written over a horizontal line.

Christina Reiss, District Judge  
United States District Court